(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－90038
（P2000－90038A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.'		識別記号	FI			テーマコード'（参考）
Ｇ０６Ｆ	13/00	３５４	Ｇ０６Ｆ	13/00	３５４Ｚ	５Ｂ０８５
	15/00	３１０		15/00	３１０Ｂ	５Ｂ０８９

審査請求　未請求　請求項の数38　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－256840

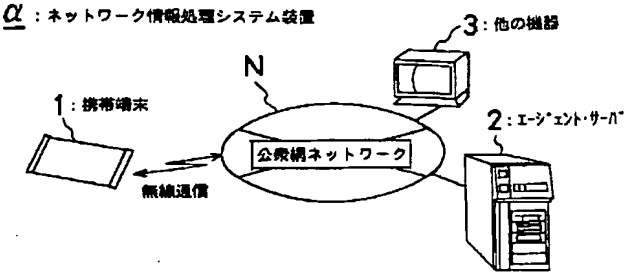
(22)出願日　平成10年９月10日(1998.9.10)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　田中　敬二
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　立道　英俊
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100071113
弁理士　菅　隆彦

最終頁に続く

(54)【発明の名称】　ネットワーク情報処理方法及びシステム装置

(57)【要約】
【課題】モバイル環境に適応した小型軽量の携帯端末を用いて高度な情報処理を行うことが可能なネットワーク情報処理方法及びシステム装置の提供。
【解決手段】携帯端末１に、当該携帯端末１の使用者を認証する個人認証手段１１と、エージェント・サーバ２における処理条件を設定する処理条件設定手段１２と、ＩＤをエージェント・サーバ２に送信するＩＤ送信手段１３と、処理条件をエージェント・サーバ２に送信する処理条件送信手段１４と、処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段１５とを具備させ、エージェント・サーバ２に、ＩＤを認証するＩＤ認証手段２１と、所要の判断及び処理並びに公衆網ネットワークＮに接続された他の機器３の管理及び制御を行う判断・処理／機器管理・制御手段２２と、処理結果を携帯端末１の処理結果受信・閲覧手段１５に送信する処理結果送信手段２３とを具備させてなる特徴。



【特許請求の範囲】
【請求項１】公衆網ネットワークに随時に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、
前記携帯端末に使用者の認証機能と処理結果表示機能を少なくとも持たせるとともに情報処理機能はすべて前記エージェント・サーバ側に持たせて簡易携帯性を高め情報処理環境の充実を計る、
ことを特徴とするネットワーク情報処理方法。
【請求項２】前記情報処理機能は、
前記エージェント・サーバ自身で賄う、
ことを特徴とする請求項１に記載のネットワーク情報処理方法。
【請求項３】前記情報処理機能は、
前記エージェント・サーバによる自分のホームサーバの起動を通して賄う、
ことを特徴とする請求項１に記載のネットワーク情報処理方法。
【請求項４】前記情報処理機能は、
前記エージェント・サーバ自身と自分のホームサーバの起動を通してその組合せで賄う、
ことを特徴とする請求項１に記載のネットワーク情報処理方法。
【請求項５】公衆網ネットワークに随意に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、
前記携帯端末は、
事前に登録された個人認証用照合データによる当該携帯端末の使用者の認証と、前記エージェント・サーバにおいて必要とされる処理条件の設定と、前記エージェント・サーバにおける処理結果の受信及び閲覧とを限定的に行い、
前記エージェント・サーバは、
前記携帯端末において設定された前記処理条件を元に、所要の判断及び処理並びに前記公衆網ネットワークに接続されかつ自己のホームサーバの起動を通して他の機器の管理及び制御を包括的に行う、ことを特徴とするネットワーク情報処理方法。
【請求項６】前記携帯端末は、
当該携帯端末の使用者の認証に代えて、当該携帯端末自身の認証を行う、
ことを特徴とする請求項１、２、３、４又は５に記載のネットワーク情報処理方法。
【請求項７】前記携帯端末は、
当該携帯端末の使用者の認証と、当該携帯端末自身の認証とを同時に行う、
ことを特徴とする請求項１、２、３、４、５又は６に記載のネットワーク情報処理方法。
【請求項８】前記エージェント・サーバは、
前記携帯端末において設定された前記処理条件を元に、前記公衆網ネットワークに接続された前記他の機器を当該公衆網ネットワークを介して制御し、
当該他の機器は、
前記エージェント・サーバからの制御により、当該処理条件に基づく前記所要の処理を実行する、
ことを特徴とする請求項５、６又は７に記載のネットワーク情報処理方法。
【請求項９】前記エージェント・サーバは、
当該エージェント・サーバにおいて得られた前記処理結果の前記携帯端末への送信に先立ち、前記所要の処理が終了した旨を示す処理終了通知を当該携帯端末に送信する、
ことを特徴とする請求項１、２、３、４、５、６、７又は８に記載のネットワーク情報処理方法。
【請求項１０】前記エージェント・サーバは、
前記携帯端末における電源のオン／オフ状態を、前記公衆網ネットワークを介して監視する、
ことを特徴とする請求項１、２、３、４、５、６、７、８又は９に記載のネットワーク情報処理方法。
【請求項１１】前記携帯端末は、
前記エージェント・サーバにおける前記所要の処理の進行状況を閲覧する、
ことを特徴とする請求項５、６、７、８、９又は１０に記載のネットワーク情報処理方法。
【請求項１２】前記携帯端末及び前記エージェント・サーバは、
それぞれ、前記公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０又は１１に記載のネットワーク情報処理方法。
【請求項１３】前記エージェント・サーバは、
前記送受信データの暗号化及び復号化に際しての暗号化／復号化方式を、前記携帯端末からの要求に応じて設定する、
ことを特徴とする請求項１２に記載のネットワーク情報処理方法。
【請求項１４】前記携帯端末の使用者の認証は、
当該携帯端末に着脱可能なＩＣカードを用いて行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２又は１３に記載のネットワーク情報処理方法。
【請求項１５】前記個人認証用照合データは、
前記携帯端末に着脱自在な前記ＩＣカード自身に登録してなる、
ことを特徴とする請求項１４に記載のネットワーク情報処理方法。
【請求項１６】前記携帯端末の使用者の認証は

パスワード入力により行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項１７】前記携帯端末の使用者の認証は、
手書き文字入力により行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項１８】前記携帯端末の使用者の認証は、
音声入力により行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項１９】前記携帯端末の使用者の認証は、
指紋入力により行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項２０】前記携帯端末の使用者の認証は、
虹彩入力により行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項２１】前記携帯端末の使用者の認証は、
パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち２以上の入力を組み合わせて行う、
ことを特徴とする請求項１、２、３、４、５、６、７、８、９、１０、１１、１２、１３、１４又は１５に記載のネットワーク情報処理方法。
【請求項２２】公衆網ネットワークに随意に接続可能な携帯端末と、前記公衆網ネットワークに定常的に接続されたエージェント・サーバとを有して構成されるネットワーク情報処理システム装置であって、
前記携帯端末は、
当該携帯端末の使用を許可された使用者を、事前に登録された個人認証用照合データに基づいて認証する個人認証手段と、前記エージェント・サーバにおいて必要とされる処理条件を設定する処理条件設定手段とで構成する認証・設定部と、
前記個人認証手段により前記使用者が適正に認証された場合に、当該使用者に付与された使用者ＩＤを前記エージェント・サーバに送信する使用者ＩＤ送信手段と、前記処理条件設定手段により設定された前記処理条件を前記エージェント・サーバに送信する処理条件送信手段とで構成するネットワーク接続部と、
前記エージェント・サーバにおける処理結果を受信して前記使用者に閲覧させる処理結果受信・閲覧手段と、を少なくとも具備し、
前記エージェント・サーバは、
前記携帯端末の前記使用者ＩＤ送信手段から送信された前記使用者ＩＤを認証する使用者ＩＤ認証手段と、この使用者ＩＤ認証手段により前記使用者ＩＤが適正に認証された場合に、前記携帯端末の前記処理条件送信手段から現在までに送信された前記処理条件を元に、所要の判断及び処理並びに前記公衆網ネットワークに接続された他の機器の管理及び制御を行う判断・処理／機器管理・制御手段とで構成する認証・設定・処理部と、
この判断・処理／機器管理・制御手段により得られた前記処理結果を前記携帯端末の前記処理結果受信・閲覧手段に送信する処理結果送信手段と、を少なくとも具備する、
ことを特徴とするネットワーク情報処理システム装置。
【請求項２３】前記ネットワーク接続部は、
前記使用者ＩＤ送信手段に代えて、
前記個人認証手段により前記使用者が適正に認証された場合に、当該携帯端末に付与された端末ＩＤを前記エージェント・サーバに送信する端末ＩＤ送信手段を具備し、
前記認証・設定・処理部は、
前記使用者ＩＤ認証手段に代えて、
前記携帯端末の当該端末ＩＤ送信手段から送信された前記端末ＩＤを認証する端末ＩＤ認証手段を具備し、
当該認証・設定・処理部の前記判断・処理／機器管理制御・手段は、
前記端末ＩＤ認証手段により前記端末ＩＤが適正に認証された場合に、所要の判断及び処理並びに前記公衆網ネットワークに接続された前記他の機器の管理及び制御を行う機能を具備する、
ことを特徴とする請求項２２に記載のネットワーク情報処理システム装置。
【請求項２４】前記ネットワーク接続部は、
前記個人認証手段により前記使用者が適正に認証された場合に、前記携帯端末に付与された端末ＩＤを前記エージェント・サーバに送信する端末ＩＤ送信手段をさらに具備し、
前記認証・設定・処理部は、
前記ネットワーク接続部の当該端末ＩＤ送信手段から送信された前記端末ＩＤを認証する端末ＩＤ認証手段をさらに具備し、
当該認証・設定・処理部の前記判断・処理／機器管理・制御手段は、
前記使用者ＩＤ認証手段及び前記端末ＩＤ認証手段により前記使用者ＩＤ及び前記端末ＩＤが共に適正に認証された場合に、所要の判断及び処理並びに前記公衆網ネットワークに接続された前記他の機器の管理及び制御を行う機能をさらに具備する、ことを特徴とする請求項２２に記載のネットワーク情報処理システム装置。
【請求項２５】前記認証・設定・処理部の前記判断・処理／機器管理・制御手段は、

前記ネットワーク接続部の前記処理条件送信手段から送信された前記処理条件を元に、前記公衆網ネットワークに接続された前記他の機器を当該公衆網ネットワークを介して制御し、当該処理条件に基づく前記所要の処理を当該他の機器に実行させる機能を具備する、
ことを特徴とする請求項２２、２３又は２４に記載のネットワーク情報処理システム装置。
【請求項２６】前記エージェント・サーバは、
前記判断・処理／機器管理・制御手段により得られた前記処理結果を前記携帯端末の前記処理結果受信・閲覧手段に送信する前に、前記所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手段に送信する処理終了通知手段をさらに具備する、
ことを特徴とする請求項２２、２３、２４又は２５に記載のネットワーク情報処理システム装置。
【請求項２７】前記エージェント・サーバは、
前記携帯端末における電源のオン／オフ状態を、前記公衆網ネットワークを介して監視する端末電源状態監視手段をさらに具備する、
ことを特徴とする請求項２２、２３、２４、２５又は２６に記載のネットワーク情報処理システム装置。
【請求項２８】前記携帯端末は、
前記エージェント・サーバにおける前記所要の処理の進行状況を閲覧する処理状況閲覧手段をさらに具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６又は２７に記載のネットワーク情報処理システム装置。
【請求項２９】前記携帯端末及び前記エージェント・サーバは、
それぞれ、前記公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う暗号化／復号化手段をさらに具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７又は２８に記載のネットワーク情報処理システム装置。
【請求項３０】前記エージェント・サーバの暗号化／復号化手段は、
前記携帯端末との間でネットワーク接続が完了したときに、前記送受信データの暗号化／復号化方式を規定するコードを設定して、当該コードを前記携帯端末の前記暗号化／復号化手段に送信する機能を具備し、
前記携帯端末の前記暗号化／復号化手段は、
前記エージェント・サーバの前記暗号化／復号化手段から送信された前記コードに対応する暗号化／復号化方式を設定する機能を具備する、
ことを特徴とする請求項２９に記載のネットワーク情報処理システム装置。
【請求項３１】前記携帯端末は、
当該携帯端末に着脱自在なＩＣカードを含んでなり、
当該ＩＣカードは、
[illegible]
認証手段を分離装備してなる、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９又は３０に記載のネットワーク情報処理システム装置。
【請求項３２】前記携帯端末に着脱自在なＩＣカードは、
前記個人認証用照合データを自身に登録する機能を具備する、
ことを特徴とする請求項３１に記載のネットワーク情報処理システム装置。
【請求項３３】前記個人認証手段は、
前記使用者の認証を実行するためのパスワード入力機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【請求項３４】前記個人認証手段は、
前記使用者の認証を実行するための手書き文字入力機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【請求項３５】前記個人認証手段は、
前記使用者の認証を実行するための音声入力機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【請求項３６】前記個人認証手段は、
前記使用者の認証を実行するための指紋入力機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【請求項３７】前記個人認証手段は、
前記使用者の認証を実行するための虹彩入力機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【請求項３８】前記個人認証手段は、
前記使用者の認証を、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち２以上の入力を組み合わせ実行する機能を具備する、
ことを特徴とする請求項２２、２３、２４、２５、２６、２７、２８、２９、３０、３１又は３２に記載のネットワーク情報処理システム装置。
【発明の詳細な説明】
【０００１】
[illegible]

処理方法及びシステム装置に関し、詳しくは、モバイル環境において、公衆網ネットワーク上のサーバとの間でネットワーク情報サービスを授受するためのネットワーク情報処理方法、及びその実施に直接使用するネットワーク情報処理システム装置に係わる。

【０００２】

【従来の技術】近年、モバイル・コンピュータなどと称される携帯端末を、アナログ電話回線やＩＳＤＮ回線（ＩＳＤＮ：サービス統合デジタル通信網）、更には携帯電話回線やＰＨＳ（Personal Handyphone System）などの公衆網からなるネットワーク（以下、単に「公衆網ネットワーク」という）に接続する。

【０００３】その携帯端末の具備する通信機能を用いて、時間や場所にとらわれることなく、インターネット接続により所望の情報の検索、閲覧を行ったり、或いは、その公衆網ネットワーク上の特定のサーバに対し情報のアップロードやダウンロードを行って、自己の情報の蓄積や、他者の情報の取出し、閲覧を行えるようになっている。また、公衆網ネットワーク上の任意の情報端末との間で、電子メールの転送を容易に行えるようになっている。

【０００４】以上のようなモバイル環境におけるネットワーク情報サービスの提供の仕組みは、公衆網ネットワークに接続され主にデータを保持したサーバと携帯端末との間で、所要のデータのやり取りを行うことが基本となっている。そして、このような形態のネットワーク情報サービスの発展に伴い、現在では、より一層の携帯性を重視し、当該サービスの授受に特化した小型軽量の携帯端末が開発されるに至っている。

【０００５】例えば、ＷｉｎｄｏｗｓＣＥ（“Ｗｉｎｄｏｗｓ”は、米マイクロソフト社登録商標）に代表される比較的規模の小さいＯＳ（オペレーティング・システム）の搭載されたＰＤＡ（Personal Digital Assistant）などが、その好例である。

【０００６】この種のＰＤＡは、上述したネットワーク情報サービスを実現するためのアプリケーション・ソフトウェア（以下、単に「アプリケーション」という）を搭載する他、通常では、例えば、スケジュール管理機能、カレンダ機能、メモ機能などといった、モバイル環境での使用に適した必要最小限の機能を実現するための簡易なアプリケーションのみを搭載している。

【０００７】なお、以上のようにネットワーク情報サービスの授受に特化したＰＤＡの他にも、Ａ５ファイル・サイズやＢ４ファイル・サイズのノート型パソコンを、携帯端末として用いる場合もある。

【０００８】この種のノート型パソコンは、処理速度が比較的速く、かつ１ＧＢ相当或いはそれ以上の記憶容量を有するデータ蓄積装置を内蔵しているため、当該ノート型パソコンによれば、例えば、Ｗｉｎｄｏｗｓ９５や９８などに代表される高度なＯＳのもと、表計算ソフト、ワープロ・ソフト、管理ソフト、ドロー・ソフトなど、そのノート型パソコンの使用者の要求に応じた高度なアプリケーションを実行できるのは勿論のこと、所要のネットワーク情報サービスの授受を行うことも可能である。

【０００９】

【発明が解決しようとする課題】ところで、上述した携帯端末のうち、ネットワーク情報サービスの授受に特化したＰＤＡでは、その記憶容量等の関係から、例えば、表計算ソフト、ワープロ・ソフト、管理ソフト、ドロー・ソフトなどといった、高度で占有プログラム容量の大きいアプリケーションの利用が事実上困難なため、モバイル環境においては、使用できるアプリケーションの種類につき制約を受けてしまう。

【００１０】また、モバイル環境に特有のアプリケーションとして、例えば、携帯端末の使用者の地図上の存在位置を、ＧＰＳ衛星（ＧＰＳ：Global Positioning System）からの電波を利用して当該携帯端末の画面上に表示し、所望により、使用者がこれから向かおうとしている目的地までの経路をリアル・タイムに案内表示する、いわゆるナビゲーション・ソフトなどの利用が考えられる。

【００１１】この種のソフトにあっては、携帯端末の使用者の移動に伴って逐次変化する位置情報に対応するために、所定の地理範囲（例えば日本全土）の全地域に及ぶ地図データを端末上に備えておく必要があり、これをＰＤＡにより行うことは、前述の記憶容量等の関係から実際上不可能である。

【００１２】これに対し、ノート型パソコンを携帯端末として用いた場合、上述のＰＤＡにおける場合のような不都合を生じることはないが、ノート型パソコンは、ＰＤＡに比べ寸法が大きく重量もあるため、本来、携帯に適するとは言いがたい面がある。

【００１３】また昨今では、急激な技術発達に伴い、ノート型パソコンの処理速度が飛躍的に向上すると共に、内蔵されるデータ蓄積装置の単位体積あたりの記憶容量も大幅に増加しているため、実際上の問題として、例えば、わずか１年前に入手したノート型パソコンのハードウェア・スペックが、現在に至り、もはや陳腐化したものとなるなどの状況を生じている。

【００１４】こうした状況のもと、ノート型パソコン上で実行されるアプリケーションの規模（プログラム容量）も年々増大する傾向にあるため、旧型（例えば、上述した１年前）のノート型パソコンでは、そのハードウェア・スペック上の制約から、こうした最新のアプリケーション（例えば、前述したナビゲーション・ソフトなど）を実行できないこともある。このようなハードウェア・スペックの陳腐化に起因する問題は、将来的にも、今後しばらくの間は続くものと予想される。

【００１５】ここにおいて、本発明の主要な目的は次の

とおりである。

【００１６】即ち、本発明の第１の目的は、モバイル環境に適応した小型軽量の携帯端末を用いながら、公衆網ネットワークを通じ高度な情報処理を行うことの可能なネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【００１７】本発明の第２の目的は、高度で占有プログラム容量の大きい様々なアプリケーションを随意に選択使用することの可能なネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【００１８】本発明の第３の目的は、使用する携帯端末のハードウェア・スペックにつき、将来にわたり陳腐化の問題の生じることのないネットワーク情報処理方法及びシステム装置を提供せんとするものである。

【００１９】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなろう。

【００２０】

【課題を解決するための手段】本発明方法においては、携帯端末に、当該携帯端末の使用者の認証、エージェント・サーバにおける処理条件の設定、エージェント・サーバにおける処理結果の受信及び閲覧などの処理を限定的に行わせ、エージェント、サーバには、携帯端末において設定された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を包括的に行わせる、という手法を講じる特徴を有する。

【００２１】また、本発明システム装置においては、携帯端末に、当該携帯端末の使用者を認証する個人認証手段と、エージェント・サーバにおける処理条件を設定する処理条件設定手段と、使用者及び／又は携帯端末に付与されたＩＤ（識別子）をエージェント・サーバに送信するＩＤ送信手段と、処理条件をエージェント・サーバに送信する処理条件送信手段と、処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段とを具備させ、エージェント・サーバには、ＩＤを認証するＩＤ認証手段と、現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う判断・処理／機器管理・制御手段と、処理結果を携帯端末の処理結果受信・閲覧手段に送信する処理結果送信手段とを具備させる、という手段を講じる特徴を有する。

【００２２】さらに、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法を採用することにより、前記目的を達成するよう為される。

【００２３】即ち、本発明方法の第1.の特徴は、公衆網ネットワークに随時に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サ[illegible]

記携帯端末に使用者の認証機能と処理結果表示機能を少なくとも持たせるとともに情報処理機能はすべて前記エージェント・サーバ側に持たせて簡易携帯性を高め情報処理環境の充実を計ってなるネットワーク情報処理方法の構成採用にある。

【００２４】本発明方法の第２の特徴は、上記本発明方法の第１の特徴における前記情報処理機能が、前記エージェント・サーバ自身で賄ってなるネットワーク情報処理方法の構成採用にある。

【００２５】本発明方法の第３の特徴は、上記本発明方法の第１の特徴における前記情報処理機能が、前記エージェント・サーバによる自分のホームサーバの起動を通して賄ってなるネットワーク情報処理方法の構成採用にある。

【００２６】本発明方法の第４の特徴は、上記本発明方法の第１の特徴における前記情報処理機能が、前記エージェント・サーバ自身と自分のホームサーバの起動を通してその組合せで賄ってなるネットワーク情報処理方法の構成採用にある。

【００２７】本発明方法の第５の特徴は、公衆網ネットワークに随意に接続可能な携帯端末と、当該公衆網ネットワークに定常的に接続されたエージェント・サーバとを用いたネットワーク情報処理をするに当り、携帯端末が、事前に登録された個人認証用照合データによる当該携帯端末の使用者の認証と、エージェント・サーバにおいて必要とされる処理条件の設定と、エージェント・サーバにおける処理結果の受信及び閲覧とを限定的に行い、エージェント・サーバが、携帯端末において設定された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続されかつ自己のホームサーバの起動を通して他の機器の管理及び制御を包括的に行ってなるネットワーク情報処理方法の構成採用にある。

【００２８】本発明方法の第６の特徴は、上記本発明方法の第１、第２、第３、第４又は第５の特徴における携帯端末が、当該携帯端末の使用者の認証に代えて、当該携帯端末自身の認証を行ってなるネットワーク情報処理方法の構成採用にある。

【００２９】本発明方法の第７の特徴は、上記本発明方法の第１、第２、第３、第４、第５又は第６の特徴における携帯端末が、当該携帯端末の使用者の認証と、当該携帯端末自身の認証とを同時に行ってなるネットワーク情報処理方法の構成採用にある。

【００３０】本発明方法の第８の特徴は、上記本発明方法の第５、第６又は第７の特徴におけるエージェント・サーバが、携帯端末において設定された処理条件を元に、公衆網ネットワークに接続された他の機器を当該公衆網ネットワークを介して制御し、当該他の機器が、エージェント・サーバからの制御により、当該処理条件に基づく所要の処理を実行してなるネットワーク情報処理[illegible]

【００３１】本発明方法の第９の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７又は第８の特徴におけるエージェント・サーバが、当該エージェント・サーバにおいて得られた処理結果の携帯端末への送信に先立ち、所要の処理が終了した旨を示す処理終了通知を当該携帯端末に送信してなるネットワーク情報処理方法の構成採用にある。

【００３２】本発明方法の第１０の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８及び第９の特徴におけるエージェント・サーバが、携帯端末における電源のオン／オフ状態を、公衆網ネットワークを介して監視してなるネットワーク情報処理方法の構成採用にある。

【００３３】本発明方法の第１１の特徴は、上記本発明方法の第５、第６、第７、第８、第９又は第１０の特徴における携帯端末が、エージェント・サーバにおける所要の処理の進行状況を閲覧してなるネットワーク情報処理方法の構成採用にある。

【００３４】本発明方法の第１２の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における携帯端末及びエージェント・サーバが、それぞれ、公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行ってなるネットワーク情報処理方法の構成採用にある。

【００３５】本発明方法の第１３の特徴は、上記本発明方法の第１２の特徴におけるエージェント・サーバが、送受信データの暗号化及び復号化に際しての暗号化／復号化方式を、携帯端末からの要求に応じて設定してなるネットワーク情報処理方法の構成採用にある。

【００３６】本発明方法の第１４の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２又は第１３の特徴における携帯端末の使用者の認証が、当該携帯端末に着脱可能なＩＣカードを用いて行ってなるネットワーク情報処理方法の構成採用にある。

【００３７】本発明方法の第１５の特徴は、上記本発明方法の第１４の特徴における個人認証用照合データが、前記携帯端末に着脱自在なＩＣカード自身に登録してなるネットワーク情報処理方法の構成採用にある。

【００３８】本発明方法の第１６の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、パスワード入力により行ってなるネットワーク情報処理方法の構成採用にある。

【００３９】本発明方法の第１７の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、手書き文字入力により行ってなるネットワーク情報処理方法の構成採用にある。

【００４０】本発明方法の第１８の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、音声入力により行ってなるネットワーク情報処理方法の構成採用にある。

【００４１】本発明方法の第１９の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、指紋入力により行ってなるネットワーク情報処理方法の構成採用にある。

【００４２】本発明方法の第２０の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、虹彩入力により行ってなるネットワーク情報処理方法の構成採用にある。

【００４３】本発明方法の第２１の特徴は、上記本発明方法の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０、第１１、第１２、第１３、第１４又は第１５の特徴における携帯端末の使用者の認証が、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち２以上の入力を組み合わせて行ってなるネットワーク情報処理方法の構成採用にある。

【００４４】一方、本発明装置の第１の特徴は、公衆網ネットワークに随意に接続可能な携帯端末と、公衆網ネットワークに定常的に接続されたエージェント・サーバとを有して構成されるネットワーク情報処理システム装置であって、携帯端末は、当該携帯端末の使用を許可された使用者を、事前に登録された個人認証用照合データに基づいて認証する個人認証手段と、エージェント・サーバにおいて必要とされる処理条件を設定する処理条件設定手段とで構成する認証・設定部と、個人認証手段により使用者が適正に認証された場合に、当該使用者に付与された使用者ＩＤをエージェント・サーバに送信する使用者ＩＤ送信手段と、処理条件設定手段により設定された処理条件をエージェント・サーバに送信する処理条件送信手段とで構成するネットワーク接続部と、エージェント・サーバにおける処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段と、を少なくとも具備し、エージェント・サーバは、携帯端末の使用者ＩＤ送信手段から送信された使用者ＩＤを認証する使用者ＩＤ認証手段と、この使用者ＩＤ認証手段により使用者ＩＤが適正に認証された場合に、携帯端末の処理条件送信手段から現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う判断・処理／機器管理・制御

手段とで構成する認証・設定・処理部と、この判断・処理／機器管理・制御手段により得られた処理結果を携帯端末の処理結果受信・閲覧手段に送信する処理結果送信手段と、を少なくとも具備してなるネットワーク情報処理システム装置の構成採用にある。

【００４５】本発明装置の第２の特徴は、上記本発明装置の第１の特徴におけるネットワーク接続部が、使用者ＩＤ送信手段に代えて、個人認証手段により使用者が適正に認証された場合に、当該携帯端末に付与された端末ＩＤをエージェント・サーバに送信する端末ＩＤ送信手段を具備し、認証・設定・処理部が、使用者ＩＤ認証手段に代えて、携帯端末の当該端末ＩＤ送信手段から送信された端末ＩＤを認証する端末ＩＤ認証手段を具備し、当該認証・設定・処理部の判断・処理／機器管理制御・手段が、端末ＩＤ認証手段により端末ＩＤが適正に認証された場合に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００４６】本発明装置の第３の特徴は、上記本発明装置の第１の特徴におけるネットワーク接続部が、個人認証手段により使用者が適正に認証された場合に、携帯端末に付与された端末ＩＤをエージェント・サーバに送信する端末ＩＤ送信手段をさらに具備し、認証・設定・処理部が、ネットワーク接続部の当該端末ＩＤ送信手段から送信された端末ＩＤを認証する端末ＩＤ認証手段をさらに具備し、当該認証・設定・処理部の判断・処理／機器管理・制御手段が、使用者ＩＤ認証手段及び端末ＩＤ認証手段により使用者ＩＤ及び端末ＩＤが共に適正に認証された場合に、所要の判断及び処理並びに公衆網ネットワークに接続された他の機器の管理及び制御を行う機能をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【００４７】本発明装置の第４の特徴は、上記本発明装置の第１、第２又は第３の特徴における認証・設定・処理部の判断・処理／機器管理・制御手段が、ネットワーク接続部の処理条件送信手段から送信された処理条件を元に、公衆網ネットワークに接続された他の機器を当該公衆網ネットワークを介して制御し、当該処理条件に基づく所要の処理を当該他の機器に実行させる機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００４８】本発明装置の第５の特徴は、上記本発明装置の第１、第２、第３又は第４の特徴におけるエージェント・サーバが、判断・処理／機器管理・制御手段により得られた処理結果を携帯端末の処理結果受信・閲覧手段に送信する前に、所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手段に送信する処理終了通知手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【００４９】本発明装置の第６の特徴は、上記本発明装置の第１、第２、第３、第４又は第５の特徴におけるエージェント・サーバが、携帯端末の電源のオン／オフ状態を、公衆網ネットワークを介して監視する端末電源状態監視手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５０】本発明装置の第７の特徴は、上記本発明装置の第１、第２、第３、第４、第５又は第６の特徴における携帯端末が、エージェント・サーバにおける所要の処理の進行状況を閲覧する処理状況閲覧手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５１】本発明装置の第８の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６又は第７の特徴における携帯端末及びエージェント・サーバが、それぞれ、公衆網ネットワークを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う暗号化／復号化手段をさらに具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５２】本発明装置の第９の特徴は、上記本発明装置の第８の特徴におけるエージェント・サーバの暗号化／復号化手段が、携帯端末との間でネットワーク接続が完了したときに、送受信データの暗号化／復号化方式を規定するコードを設定して、当該コードを携帯端末の暗号化／復号化手段に送信する機能を具備し、携帯端末の暗号化／復号化手段が、エージェント・サーバの暗号化／復号化手段から送信されたコードに対応する暗号化／復号化方式を設定する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５３】本発明装置の第１０の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８又は第９の特徴における携帯端末が、当該携帯端末に着脱自在なＩＣカードを含んでなり、当該ＩＣカードが、当該携帯端末の各構成手段のうち、少なくとも個人認証手段を分離装備してなるネットワーク情報処理システム装置の構成採用にある。

【００５４】本発明装置の第１１の特徴は、上記本発明装置の第１０の特徴における携帯端末に着脱自在なＩＣカードが、個人認証用照合データを自身に登録する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５５】本発明装置の第１２の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における個人認証手段が、使用者の認証を実行するためのパスワード入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５６】本発明装置の第１３の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第

段が、使用者の認証を実行するための手書き文字入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５７】本発明装置の第１４の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における個人認証手段が、使用者の認証を実行するための音声入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５８】本発明装置の第１５の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における個人認証手段が、使用者の認証を実行するための指紋入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００５９】本発明装置の第１６の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における個人認証手段が、使用者の認証を実行するための虹彩入力機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００６０】本発明装置の第１７の特徴は、上記本発明装置の第１、第２、第３、第４、第５、第６、第７、第８、第９、第１０又は第１１の特徴における個人認証手段が、使用者の認証を、パスワード入力、手書き文字入力、音声入力、指紋入力及び虹彩入力のうち２以上の入力を組み合わせ実行する機能を具備してなるネットワーク情報処理システム装置の構成採用にある。

【００６１】

【発明の実施の形態】以下、添付図面を参照しつつ、本発明の実施の形態を、その第１及び第２装置例及びこれらに対応する第１及び第２方法例につき説明する。

【００６２】（第１装置例）図１は、本装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。また、図２は、本装置例に係るネットワーク情報処理システム装置における携帯端末及びエージェント・サーバの機能構成を示すブロック図である。

【００６３】まず、図１に示すように、この第１装置例に係るネットワーク情報処理システム装置αは、基本的に、公衆網ネットワークＮに随意に接続可能な携帯端末１と、公衆網ネットワークに定常的に接続されたエージェント・サーバ２とを有して構成され、これらに加え、公衆網ネットワークＮには、会社や家庭に設置されたパソコンなどの情報端末や、或いは、情報端末として機能するテレビ受像機などの他の機器３が接続できるようになっている。

【００６４】なお、公衆網ネットワークＮと携帯端末１との接続形態は任意であるが、この第１装置例では、無線通信を用いる携帯電話回線やＰＨＳなどによって、所要のネットワーク接続を行う例を示している。

【００６５】次に、図２に示すように、携帯端末１は、基本的に、当該携帯端末１の使用を許可された使用者を、事前に登録された個人認証用照合データに基づいて認証する個人認証手段１１と、エージェント・サーバ２において必要とされる処理条件を設定する処理条件設定手段１２とからなる認証・設定部１ａと、個人認証手段１１により使用者が適正に認証された場合に、当該使用者に付与された使用者ＩＤ及び／又は携帯端末１に付与された端末ＩＤをエージェント・サーバ２に送信する使用者ＩＤ／端末ＩＤ送信手段１３と、処理条件設定手段１２により設定された処理条件をエージェント・サーバ２に送信する処理条件送信手段１４とからなるネットワーク接続部１ｂと、エージェント・サーバ２における処理結果を受信して使用者に閲覧させる処理結果受信・閲覧手段１５とを具備して構成される。

【００６６】なお、上述の個人認証手段１１としては、所要の使用者の認証を、例えば、パスワード入力により行うもの、手書き文字入力により行うもの、音声入力により行うもの、指紋入力により行うもの、虹彩入力により行うものなどが挙げられるが、その適用に際しては、これら各入力を単独で用いたり、或いは、２以上の入力を組み合わせて用いるようにしてもよい。

【００６７】また、携帯端末１には、以上の各手段他、エージェント・サーバ２における所要の処理の進行状況を閲覧する処理状況閲覧手段１６を具備させてもよい。

【００６８】一方、エージェント・サーバ２は、基本的に、携帯端末１の使用者ＩＤ／端末ＩＤ送信手段１３から送信された使用者ＩＤ及び／又は端末ＩＤを認証する使用者ＩＤ／端末ＩＤ認証手段２１と、この使用者ＩＤ／端末ＩＤ認証手段２１により使用者ＩＤ及び／又は端末ＩＤが適正に認証された場合に、携帯端末１の処理条件送信手段１２から現在までに送信された処理条件を元に、所要の判断及び処理並びに公衆網ネットワークＮに接続されかつ自分のホームサーバの起動を通して他の機器３の管理及び制御を行う判断・処理／機器管理・制御手段２２とからなる認証・設定・処理部２ａと、この判断・処理／機器管理・制御手段２２により得られた処理結果を携帯端末１の処理結果受信・閲覧手段１５に送信する処理結果送信手段２３とを具備して構成される。

【００６９】なお、判断・処理／機器管理・制御手段２２は、携帯端末１の処理条件送信手段１４から送信された処理条件を元に、公衆網ネットワークＮに接続された他の機器３を当該公衆網ネットワークＮを介して制御し、当該処理条件に基づく所要の処理を当該他の機器３に実行させることも可能である。

【００７０】また、エージェント・サーバ２に対しても、以上の各手段の他、判断・処理／機器管理・制御手段２１により得られた処理結果を携帯端末１の処理結果受信・閲覧手段１５に送信する前に、所要の処理が終了した旨を示す処理終了通知を当該処理結果受信・閲覧手

段１５に送信する処理終了通知手段２４を具備させたり、或いは、携帯端末１の電源のオン／オフ状態を、公衆網ネットワークＮを介して監視する端末電源状態監視手段２５を具備させてもよい。

【００７１】さらに、携帯端末１及びエージェント・サーバ２の両者には、それぞれ、公衆網ネットワークＮを介し双方間でやり取りされる送受信データの暗号化及び復号化を行う暗号化／復号化手段（図示せず）を具備させてもよい。

【００７２】ここで、エージェント・サーバ２の暗号化／復号化手段には、携帯端末１との間でネットワーク接続が完了したときに、送受信データの暗号化／復号化方式を規定するコードを設定させて、当該コードを携帯端末１の暗号化／復号化手段に送信させ、これに対し、携帯端末１の暗号化／復号化手段には、エージェント・サーバ２の暗号化／復号化手段から送信されたコードに対応する暗号化／復号化方式を設定させるようにすればよい。

【００７３】（第１方法例）次に、以上のように構成された第１装置例に係るネットワーク情報処理システム装置αに適用される第１方法例につき説明する。

【００７４】まず、携帯端末１においてネットワーク情報サービスを授受するために、当該携帯端末１の認証・設定部１ａにおいては、例えば、指紋認証装置（図示せず）などの個人認証手段１１により、当該サービスを受けようとする個人を認証し、当該サービスを受けるためのエージェント・サーバ２における処理条件を、処理条件設定手段１２により設定する。

【００７５】その後、携帯端末１のネットワーク接続部１ｂは、エージェント・サーバ２との間で公衆網ネットワークＮを介したネットワーク接続を行い、使用者ＩＤ及び／又は端末ＩＤを、使用者ＩＤ／端末ＩＤ送信手段１３によってエージェント・サーバ２に送信することにより、当該エージェント・サーバ２の認証・設定・処理部２ａにおいては、自己の管理している過去の蓄積データを元に、使用者ＩＤ／端末ＩＤ認証手段２１において使用者及び／又は携帯端末を特定して認証することができ、これによりネットワーク情報サービスの提供の可否が判断される。

【００７６】そして、このようにしてネットワーク情報サービスの提供が許容されると、携帯端末１のネットワーク接続部１ｂは、エージェント・サーバ２における処理条件を、処理条件送信手段１４によって送信し、これを受信した当該エージェント・サーバ２の認証・設定・処理部２ａにおける判断・処理／機器管理・制御手段２２は、携帯端末１から要求されている処理内容を把握して、判断、設定、処理、管理、或いは、他の機器３を制御するようにとの各種命令に対する所要の処理を実行する。

【００７７】なお、携帯端末１においては、エージェント・サーバ２の処理結果送信手段２３により、当該エージェント・サーバ２における処理結果を通信で受け取ることができ、さらに処理結果受信・閲覧手段１５により、その処理結果を閲覧することができる。

【００７８】そして、このような一連の処理が、ネットワーク情報処理システム装置α内で行われることにより、高度な処理プログラムが動作しない軽微な携帯端末１であっても、高度な処理結果を得ることが可能となる。

【００７９】なお、エージェント・サーバ２に処理終了通知手段２４を具備させることにより、携帯端末１の利用者は、処理結果受信・閲覧手段１５により、エージェント・サーバ２における所要の処理が終了したことを瞬時に知ることができ、この処理終了通知手段２４により、一層利用しやすいネットワーク情報処理システム装置αを構築することができる。

【００８０】この処理終了通知手段２４の動作につき、具体的には、エージェント・サーバ２が携帯端末１から処理を依頼された場合に、当該携帯端末１から端末ＩＤを受け取って、その携帯端末１を認識した後に所要の処理を実行するようにし、その処理が終了した時点で、認識した携帯端末１の端末ＩＤを元に、その携帯端末１に対し終了通知を発信するようにするとよい。

【００８１】また、エージェント・サーバ２に端末電源状態監視手段２５を具備させることにより、携帯端末１の電源がオフ状態のときに、不要な処理終了通知を送信しなくても済むようになるメリットがある。

【００８２】この端末電源状態監視手段２５の動作につき、具体的には、携帯端末１の電源がオン状態となっているときに、端末ＩＤなど当該携帯端末１を特定できる情報を含んだ電波を、その携帯端末１に連続的又は断続的に発信させておき、この電波を、無線基地局（図示せず）から公衆網ネットワークＮを介してエージェント・サーバ２に送信することにより、当該携帯端末１の電源のオン／オフ状態を監視させるようにするとよい。

【００８３】さらに、携帯端末１に処理状況閲覧手段１６を具備させることにより、エージェント・サーバ２において実行中の処理の終了に時間がかかるものと見込まれる場合に、その処理が終了する前に、当該処理の変更（強制終了など）を行うことができるなどのメリットがある。

【００８４】この処理状況閲覧手段１６の動作につき、具体的には、携帯端末１から処理状況確認メッセージが無線により送信させて、そのメッセージを受け取ったエージェント・サーバ２に、そのときの処理状況を携帯端末１に送信させるようにするとよい。

【００８５】さらにまた、携帯端末１及びエージェント・サーバ２の両者に暗号化／復号化手段を具備させることにより、双方間の送受信データが第三者に不正に受信されて利用されるのを、防止できるメリットがある。

【００８６】（第２装置例）続いて、図３は、本装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【００８７】同図に示すように、この本装置例に係るネットワーク情報処理システム装置βは、前記第１装置例におけるそれと同様、基本的に、公衆網ネットワークＮに随意に接続可能な携帯端末１と、公衆網ネットワークに定常的に接続されたエージェント・サーバ２とを有して構成され、携帯端末１が、当該端末に着脱自在なＩＣカード４を含んでなり、当該ＩＣカード４が、携帯端末１の構成手段に含まれる個人認証手段１１を分離装備すると共に、個人認証用照合データを自身に登録したものとなっている。

【００８８】また、このＩＣカード４は、公衆網ネットワークＮに接続された他の端末５に対しても装着自在に構成することが可能である。（ＩＣカード４自身の構成については、本願出願人による特願平１０－１４４８８５号に詳しい。）

【００８９】（第２方法例）次に、以上のように構成された第２装置例に係るネットワーク情報処理システム装置βに適用される第２方法例につき説明する。

【００９０】個人認証をＩＣカード４により行う場合、当該ＩＣカード４には、個人認証用照合データは勿論、個人が受けられるネットワーク情報サービスの種類に関するデータを保存しておくようにする。

【００９１】このＩＣカード４を用いたネットワーク情報処理システム装置βにおいては、携帯端末１における個人認証がＩＣカード４内のデータに基づいて行われる以外は、図２のブロック図に示した各構成手段により実現される機能と同様な機能を有するが、当該ＩＣカード４によって、個人認証とネットワーク情報サービスの設定が行えるようになるため、図示の他の端末５を用いて、同様に高度なネットワーク情報サービスを受けようとする場合、そのＩＣカード４のみを持ち運べば済むというメリットがある。

【００９２】また、このＩＣカード４に、例えば指紋認証装置などの個人認証手段１１を、携帯端末１とは独立して具備させることにより、当該携帯端末１における個人認証処理が不要となって、その携帯端末１の装備を、一層軽微にすることができるというメリットがある。

【００９３】

【実施例】続いて、実施例として、本実施形態を利用してネットワーク情報サービスを受ける場合の一連の手順について説明する。

【００９４】本発明によりネットワーク情報サービスを受けるためには、携帯端末１の使用者が、利用したいサービスの種類をエージェント・サーバ２を保有するプロバイダ（図示せず）に申請し、当該サービスを新規に登録するための「サービス新規登録」と、携帯端末１の使用者が、既に利用登録済みの当該サービスの利用環境を設定し、そのときの設定情報をプロバイダに通知するための「サービス環境設定」とを行い、その後に、実際の「サービス利用」が可能となる。

【００９５】以下、これら各フローを、第１装置例及びこれに適用する第１方法例における場合（ＩＣカード不要）と、並びに第２装置例及びこれに適用する第２方法例における場合（ＩＣカード要）とにつき順に説明する。

【００９６】＜ＩＣカード不要のサービス新規登録＞図４は、ＩＣカード不要のサービス新規登録の手順を説明するためのフローチャートである。

【００９７】ＩＣカード４不要のサービス新規登録に際しては、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求して（ＳＴ１）、当該使用者ＩＤの投入後にローカル個人認証を行う（ＳＴ２）。

【００９８】ここで、投入された使用者ＩＤが適正なものであるか否かを判定するが（ＳＴ３）、それが、既に携帯端末１に登録されているユーザ情報と一致しない場合（ＳＴ３；ＮＯ）、携帯端末１は、ローカル個人認証が失敗したとして、当該携帯端末１の利用者に対し登録不可通知を提示して（ＳＴ４）、処理を終了する。

【００９９】これに対し、投入された使用者ＩＤが携帯端末１に登録されているユーザ情報と一致した場合（ＳＴ３；ＹＥＳ）には、携帯端末１は、エージェント・サーバ２に対し当該使用者ＩＤを送信し（ＳＴ５）、以下、当該エージェント・サーバ２において、その使用者ＩＤのチェックを行って（ＳＴ６）、これが適正な使用者ＩＤであるか否かを判定する（ＳＴ７）。

【０１００】この判定の結果、送信されてきた使用者ＩＤが不適正なものである場合（ＳＴ７；ＮＯ）には、新規サービスの利用が不可であるとして、前述のＳＴ４の処理において、当該携帯端末１の利用者に対し登録不可通知を提示して処理を終了するが、それが適正なものである場合（ＳＴ７；ＹＥＳ）、エージェント・サーバ２は、新規サービスの利用が可能であるとして、当該新規サービスに対する利用者ＩＤを登録し（ＳＴ８）、以下、携帯端末１に、その登録が完了した旨を通知すると共に（ＳＴ９）、当該携帯端末１において所要のサービスＩＤを記入して（ＳＴ１０）、全ての処理を終了する。

【０１０１】＜ＩＣカード不要のサービス環境設定＞図５は、ＩＣカード不要のサービス環境設定の手順を説明するためのフローチャートである。

【０１０２】ＩＣカード４不要のサービス環境設定に際しては、上述のサービス新規登録と同様に、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求して（ＳＴ１１）、当該使用者ＩＤの投入後にローカル個人認証を行う（ＳＴ１２）。

【０１０３】ここで、投入された使用者ＩＤが適正なものであるか否かを判定するが（ＳＴ１３）、それが、既

に携帯端末１に登録されているユーザ情報と一致しない場合（ＳＴ１３；ＮＯ）、携帯端末１は、上述のサービス新規登録と同様、ローカル個人認証が失敗したとして、当該携帯端末１の利用者に対し登録不可通知を提示して（ＳＴ１４）、処理を終了する。

【０１０４】これに対し、投入された使用者ＩＤが携帯端末１に登録されているユーザ情報と一致した場合（ＳＴ１３；ＹＥＳ）には、携帯端末１は、所要のサービス利用環境の設定を行った後に（ＳＴ１５）、エージェント・サーバ２に対し、使用者ＩＤと当該サービス利用環境を送信し（ＳＴ１６）、以下、当該エージェント・サーバ２において、そのサービス利用環境のチェックを行って（ＳＴ１７）、これが適正なサービス利用環境であるか否かを判定する（ＳＴ１８）。

【０１０５】この判定の結果、送信されてきたサービス利用環境が不適正なものである場合（ＳＴ１８；ＮＯ）には、前述のＳＴ１４の処理において、当該携帯端末１の利用者に対し登録不可通知を提示して処理を終了するが、それが適正なものである場合（ＳＴ１８；ＹＥＳ）、エージェント・サーバ２は、サービス利用環境の設定登録を行って（ＳＴ１９）、携帯端末１に、その設定登録が完了した旨を通知すると共に（ＳＴ２０）、当該携帯端末１において所要のサービス利用環境データを書き込んで（ＳＴ２１）、全ての処理を終了する。

【０１０６】＜ＩＣカード不要のサービス利用＞図６及び図７は、ＩＣカード不要のサービス利用のそれぞれ前半及び後半の手順を説明するためのフローチャートである。なお、本図では、携帯端末１の使用者の位置情報をエージェント・サーバ２が捕捉し、当該使用者の現在位置を表した周辺地図を携帯端末１へ転送するサービスの利用について説明する。

【０１０７】ＩＣカード４不要のサービス利用（進路ナビゲーション・サービス）に際しては、上述のサービス新規登録及び環境設定と同様に、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求して（ＳＴ３１）、当該使用者ＩＤの投入後にローカル個人認証を行う（ＳＴ３２）。

【０１０８】ここで、投入された使用者ＩＤが適正なものであるか否かを判定するが（ＳＴ３３）、それが、既に携帯端末１に登録されているユーザ情報と一致しない場合（ＳＴ３３；ＮＯ）、携帯端末１は、上述のサービス新規登録及び環境設定と同様、ローカル個人認証が失敗したとして、当該携帯端末１の利用者に対し登録不可通知を提示して（ＳＴ３４）、処理を終了する。

【０１０９】これに対し、投入された使用者ＩＤが携帯端末１に登録されているユーザ情報と一致した場合（ＳＴ３３；ＹＥＳ）には、携帯端末１は、エージェント・サーバ２に対し、当該使用者ＩＤと、前述のサービス新規登録の処理で携帯端末１に記入したサービスＩＤとを送信し（ＳＴ３５）、以下、当該エージェント・サーバ２において、その使用者ＩＤ及びサービスＩＤのチェックを行って（ＳＴ３６）、これが適正なサービス利用環境であるか否かを判定する（ＳＴ３７）。

【０１１０】この判定の結果、送信されてきた使用者ＩＤ及びサービスＩＤが不適正なものである場合（ＳＴ３７；ＮＯ）には、前述のＳＴ３４の処理において、当該携帯端末１の利用者に対しサービス不可通知を提示して処理を終了するが、それらが適正なものである場合（ＳＴ３７；ＹＥＳ）には、携帯端末１の使用者へのサービス許可通知及び待機要求を行う（ＳＴ３８）。なお、このとき携帯端末１は、通信待ち受け状態となっている。

【０１１１】その後、エージェント・サーバ２では、携帯端末１の使用者の位置情報を捕捉し（ＳＴ３９）、例えば、携帯端末１の使用者の現在位置を表した地図情報を作成するなどといった出力情報処理を行った後に（ＳＴ４０）、その携帯端末１に対し処理終了通知を送信する（ＳＴ４１）。

【０１１２】これに対し、携帯端末１では、送信されてきた処理終了通知を表示し（ＳＴ４２）、再びローカル個人認証を行う（ＳＴ４３）。

【０１１３】ここで、再び投入された使用者ＩＤが適正なものであるか否かを判別するが（ＳＴ４４）、それが、これまでに携帯端末１に登録されているユーザ情報と一致しない場合（ＳＴ４４；ＮＯ）、携帯端末１は、その使用者から誤った使用者ＩＤが入力されたとして、再び、当該携帯端末１の使用者に対し個人認証を要求して（ＳＴ４５）、前述のＳＴ４３のローカル個人認証を繰り返し行う。

【０１１４】これに対し、投入された使用者ＩＤが携帯端末１に登録されているユーザ情報と一致した場合（ＳＴ４４；ＹＥＳ）、エージェント・サーバ２は、携帯端末１に対し処理結果を送信し（ＳＴ４６）、以下、携帯端末１においては、当該処理結果の受信・閲覧表示を行った後に（ＳＴ４７）、エージェント・サーバ２に受信完了通知を送信し（ＳＴ４８）、これにより全ての処理を終了する。

【０１１５】続いて、ＩＣカード４を使用したときのサービス提供について説明する。

【０１１６】＜ＩＣカード要のサービス新規登録＞図８は、ＩＣカード要のサービス新規登録の手順を説明するためのフローチャートである。

【０１１７】ＩＣカード４要のサービス新規登録に際しては、その未使用時における場合と同様、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求するが（ＳＴ５１）、当該使用者ＩＤの投入後のローカル個人認証（ＳＴ５２）及びその使用者ＩＤの判定（ＳＴ５３）は、携帯端末１ではなく、ＩＣカード４において行う。

【０１１８】そして、再び携帯端末１において、投入された使用者ＩＤがユーザ情報と一致しない場合（ＳＴ５

３；ＮＯ）には、当該携帯端末１の利用者に対し登録不可通知を提示し（ＳＴ５４）、一致した場合（ＳＴ５３；ＹＥＳ）には、エージェント・サーバ２に対し当該使用者ＩＤを送信し（ＳＴ５５）、以下、当該エージェント・サーバ２において、使用者ＩＤのチェック（ＳＴ５６）及びその判定（ＳＴ５７）を行う。

【０１１９】以下、同様に、送信されてきた使用者ＩＤが不適正なものである場合（ＳＴ５７；ＮＯ）には、携帯端末１の利用者に対し登録不可通知を提示し、それが適正なものである場合（ＳＴ５７；ＹＥＳ）には、エージェント・サーバ２は、新規サービスに対する利用者ＩＤを登録し（ＳＴ５８）、さらに、携帯端末１に、その登録が完了した旨を通知する（ＳＴ５９）。

【０１２０】そして、以上の処理の終了と共に、携帯端末１の制御の下、ＩＣカード４に所要のサービスＩＤを記入し（ＳＴ６０）、これにより全ての処理を終了する。

【０１２１】＜ＩＣカード要のサービス環境設定＞図９は、ＩＣカード要のサービス環境設定の手順を説明するためのフローチャートである。

【０１２２】ＩＣカード４要のサービス環境設定に際しては、その未使用時における場合と同様、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求するが（ＳＴ６１）、当該使用者ＩＤの投入後のローカル個人認証（ＳＴ６２）及びその使用者ＩＤの判定（ＳＴ６３）は、携帯端末１ではなく、ＩＣカード４において行う。

【０１２３】そして、再び携帯端末１において、投入された使用者ＩＤがユーザ情報と一致しない場合（ＳＴ６３；ＮＯ）には、当該携帯端末１の利用者に対し登録不可通知を提示し（ＳＴ６４）、一致した場合（ＳＴ６３；ＹＥＳ）には、サービス利用環境の設定を行った後に（ＳＴ６５）、エージェント・サーバ２に対し、使用者ＩＤと当該サービス利用環境を送信し（ＳＴ６６）、以下、当該エージェント・サーバ２において、そのサービス利用環境のチェック（ＳＴ６７）及びその判定（ＳＴ６８）を行う。

【０１２４】以下、同様に、送信されてきたサービス利用環境が不適正なものである場合（ＳＴ６８；ＮＯ）には、当該携帯端末１の利用者に対し登録不可通知を提示し、それが適正なものである場合（ＳＴ６８；ＹＥＳ）、エージェント・サーバ２は、サービス利用環境の設定登録を行って（ＳＴ６９）、携帯端末１に、その設定登録が完了した旨を通知する（ＳＴ７０）。

【０１２５】そして、以上の処理の終了と共に、携帯端末１の制御の下、ＩＣカード４に所要のサービス利用環境データを書き込み（ＳＴ７１）、これにより全ての処理を終了する。

【０１２６】＜ＩＣカード要のサービス利用＞図１０及び図１１は、ＩＣカード要の[illegible]利用のための前半及び後半の手順を説明するためのフローチャートである。なお、本図においても、前述の進路ナビゲーション・サービスについて説明する。

【０１２７】ＩＣカード４要のサービス利用に際しては、その不要の場合と同様、まず、携帯端末１から、その使用者に対して使用者ＩＤの投入を要求するが（ＳＴ８１）、当該使用者ＩＤの投入後にローカル個人認証（ＳＴ８２）及びその使用者ＩＤの判定（ＳＴ８３）は、携帯端末１ではなく、ＩＣカード４において行う。

【０１２８】そして、再び携帯端末１において、その使用者ＩＤがユーザ情報と一致しない場合（ＳＴ８３；ＮＯ）には、携帯端末１は、当該携帯端末１の利用者に対しサービス不可通知を提示し（ＳＴ８４）、一致した場合（ＳＴ８３；ＹＥＳ）には、エージェント・サーバ２に対し、当該使用者ＩＤと、前述のサービス新規登録の処理で携帯端末１に記入したサービスＩＤとを送信し（ＳＴ８５）、以下、当該エージェント・サーバ２において、その使用者ＩＤ及びサービスＩＤのチェック（ＳＴ８６）及びその判定する（ＳＴ８７）を行う。

【０１２９】そして、送信されてきた使用者ＩＤ及びサービスＩＤが不適正なものである場合（ＳＴ８７；ＮＯ）には、当該携帯端末１の利用者に対しサービス不可通知を提示し、それらが適正なものである場合（ＳＴ８７；ＹＥＳ）、エージェント・サーバ２は、携帯端末１の使用者へのサービス許可通知及び待機要求（ＳＴ８８）、並びに携帯端末１の使用者の位置情報の捕捉（ＳＴ８９）を順次行い、さらに出力情報処理を行った後に（ＳＴ９０）、その携帯端末１に対し処理終了通知を送信する（ＳＴ９１）。

【０１３０】これに対し、携帯端末１では、送信されてきた処理終了通知を表示するが（ＳＴ９２）、続くローカル個人認証（ＳＴ９３）及びその判別（ＳＴ９４）並びに個人認証の要求（ＳＴ９５）については、携帯端末１ではなく、ＩＣカード４において行う。

【０１３１】そして、エージェント・サーバ２は、携帯端末１に対し処理結果を送信し（ＳＴ９６）、以下、携帯端末１において、当該処理結果の受信・閲覧表示を行った後に（ＳＴ９７）、エージェント・サーバ２に受信完了通知を送信し（ＳＴ９８）、これにより全ての処理を終了する。

【０１３２】以上、本発明の実施の形態及び実施例につき説明したが、本発明は、必ずしも上述した手段及び手法にのみ限定されるものではなく、本発明にいう目的を達成し、後述する効果を有する範囲内において、適宜、変更実施することが可能なものである。

【０１３３】

【発明の効果】以上説明したように、本発明によれば、モバイル環境に適応した小型軽量の携帯端末を用いながら、公衆網ネットワークを通じ高度な情報処理を行うこと[illegible]

きい様々なアプリケーションを随意に選択使用することが可能となり、加えて、使用する携帯端末のハードウェア・スペックにつき、将来にわたり陳腐化の問題を生じることがなくなる。

【図面の簡単な説明】

【図１】本発明の実施の形態を示す第１装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【図２】同上における携帯端末及びエージェント・サーバの機能構成を示すブロック図である。

【図３】本発明の実施の形態を示す第２装置例に係るネットワーク情報処理システム装置のネットワーク構成を示す図である。

【図４】本発明の実施の形態の実施例を示すＩＣカード不要のサービス新規登録の手順を説明するためのフローチャートである。

【図５】同上、サービス環境設定の手順を説明するためのフローチャートである。

【図６】同上、サービス利用の前半の手順を説明するためのフローチャートである。

【図７】同上、サービス利用の後半の手順を説明するためのフローチャートである。

【図８】本発明の実施の形態の実施例を示すＩＣカード要のサービス新規登録の手順を説明するためのフローチャートである。

【図９】同上、サービス環境設定の手順を説明するためのフローチャートである。

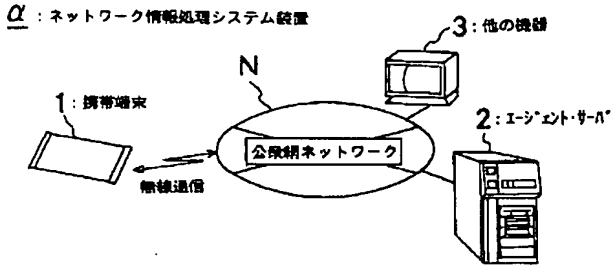
【図１０】同上、サービス利用の前半の手順を説明するためのフローチャートである。

【図１１】同上、サービス利用の後半の手順を説明するためのフローチャートである。

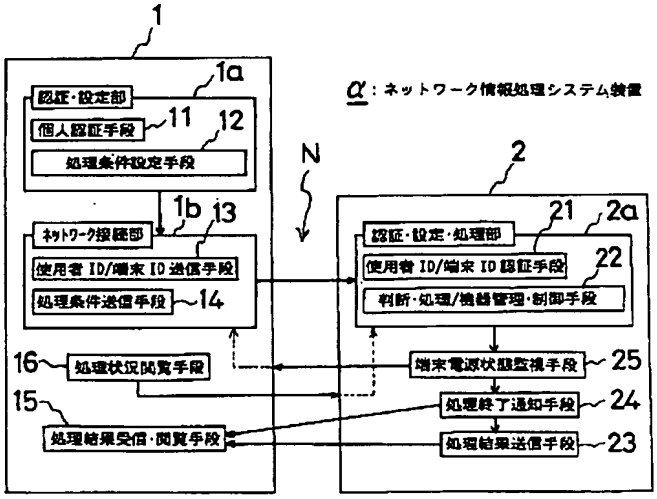
【符号の説明】

α，β…ネットワーク情報処理システム装置
Ｎ…公衆網ネットワーク
１…携帯端末
１ａ…認証・設定部
１ｂ…ネットワーク接続部
１１…個人認証手段
１２…処理条件設定手段
１３…使用者ＩＤ／端末ＩＤ送信手段
１４…処理条件送信手段
１５…処理結果受信・閲覧手段
１６…処理状況閲覧手段
２…エージェント・サーバ
２ａ…認証・設定・処理部
２１…使用者ＩＤ／端末ＩＤ認証手段
２２…判断・処理／機器管理・制御手段
２３…処理結果送信手段
２４…処理終了通知手段
２５…端末電源状態監視手段
３…他の機器
４…ＩＣカード
５…他の端末

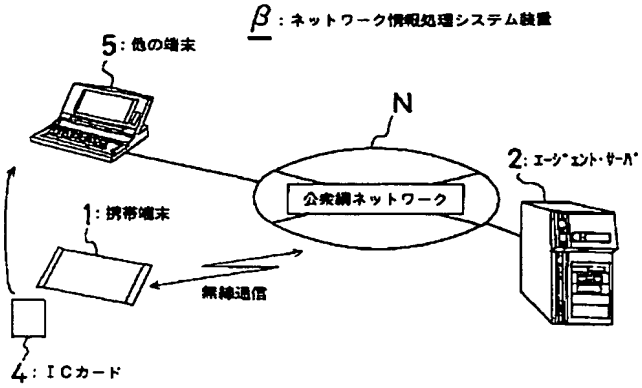
【図１】



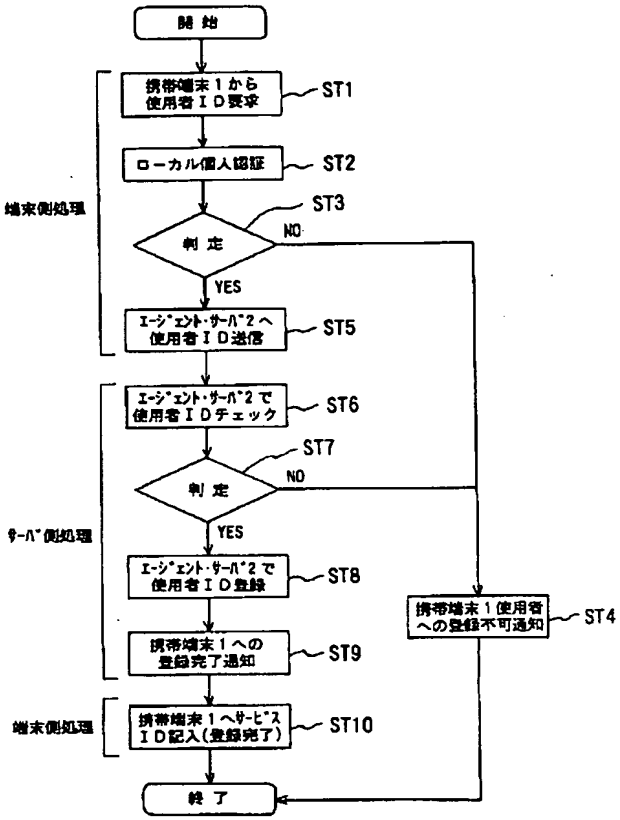
【図２】



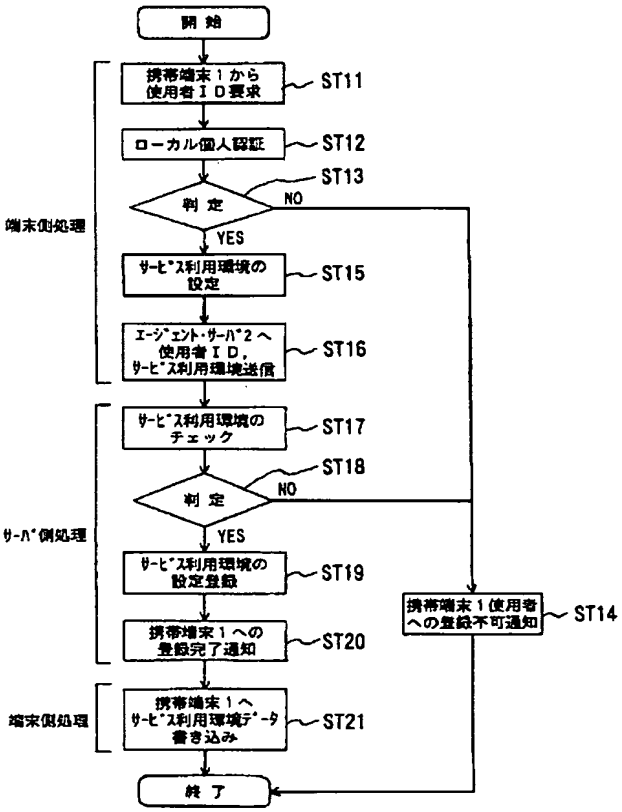
【図３】


β：ネットワーク情報処理システム装置
5：他の端末
N
2：ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ
公衆網ネットワーク
1：携帯端末
無線通信
4：ＩＣカード

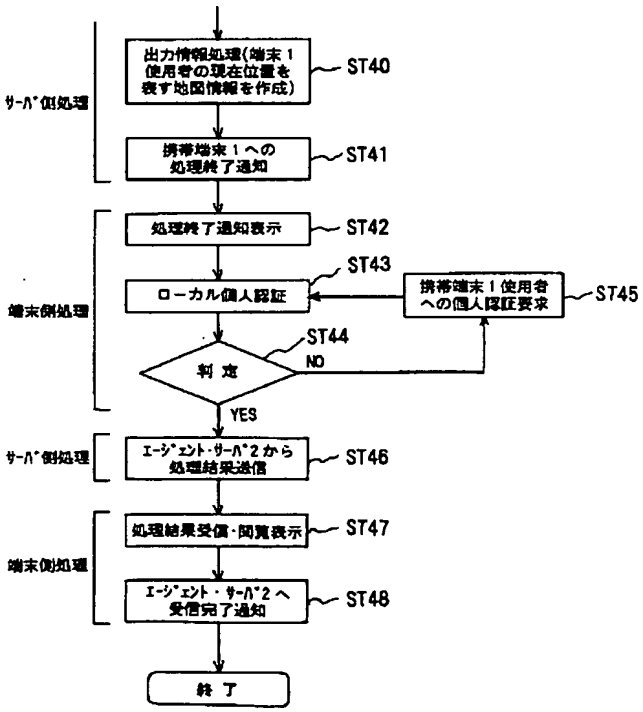
【図４】


開 始
携帯端末１から使用者ＩＤ要求
ST1
ローカル個人認証
ST2
判 定
ST3
NO
YES
端末側処理
ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ2へ使用者ＩＤ送信
ST5
ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ2で使用者ＩＤチェック
ST6
判 定
ST7
NO
YES
ｻｰﾊﾞ側処理
ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ2で使用者ＩＤ登録
ST8
携帯端末１への登録完了通知
ST9
携帯端末１使用者への登録不可通知
ST4
携帯端末１へｻｰﾋﾞｽＩＤ記入(登録完了)
ST10
端末側処理
終 了

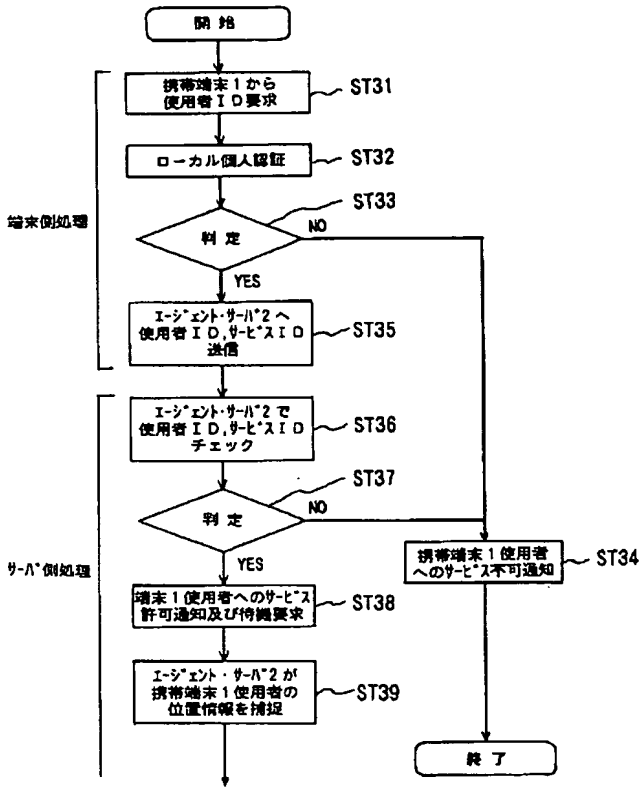
【図５】


開 始
携帯端末１から使用者ＩＤ要求
ST11
ローカル個人認証
ST12
判 定
ST13
NO
YES
端末側処理
ｻｰﾋﾞｽ利用環境の設定
ST15
ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ2へ使用者ＩＤ，ｻｰﾋﾞｽ利用環境送信
ST16
ｻｰﾋﾞｽ利用環境のチェック
ST17
判 定
ST18
NO
YES
ｻｰﾊﾞ側処理
ｻｰﾋﾞｽ利用環境の設定登録
ST19
携帯端末１への登録完了通知
ST20
携帯端末１使用者への登録不可通知
ST14
携帯端末１へｻｰﾋﾞｽ利用環境ﾃﾞｰﾀ書き込み
ST21
端末側処理
終 了

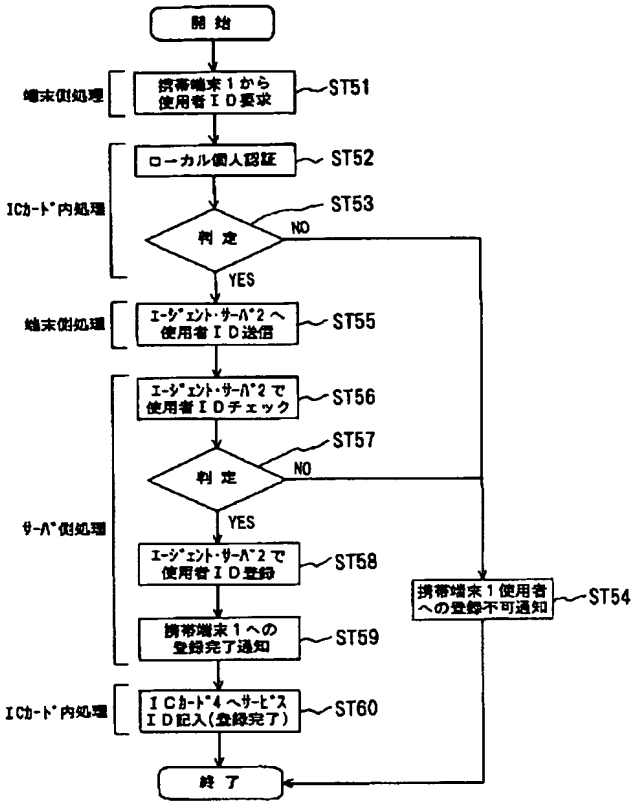
【図７】


出力情報処理(端末１使用者の現在位置を表す地図情報を作成)
ST40
ｻｰﾊﾞ側処理
携帯端末１への処理終了通知
ST41
処理終了通知表示
ST42
ローカル個人認証
ST43
携帯端末１使用者への個人認証要求
ST45
判 定
ST44
NO
YES
端末側処理
ｴｰｼﾞｪﾝﾄ･ｻｰﾊﾞ2から処理結果送信
ST46
ｻｰﾊﾞ側処理
処理結果受信･閲覧表示
ST47
ｴｰｼﾞｪﾝﾄ・ｻｰﾊﾞ2へ受信完了通知
ST48
端末側処理
終 了

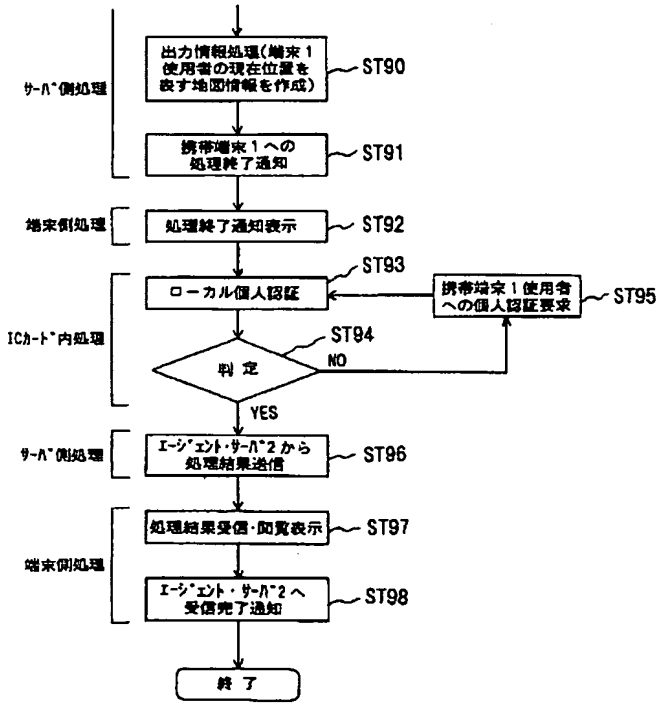
【図６】


開始
携帯端末１から使用者ＩＤ要求
ST31
ローカル個人認証
ST32
判定
ST33
NO
YES
エージェント・サーバ２へ使用者ＩＤ,サービスＩＤ送信
ST35
エージェント・サーバ２で使用者ＩＤ,サービスＩＤチェック
ST36
判定
ST37
NO
YES
携帯端末１使用者へのサービス不可通知
ST34
端末１使用者へのサービス許可通知及び待機要求
ST38
エージェント・サーバ２が携帯端末１使用者の位置情報を捕捉
ST39
終了
端末側処理
サーバ側処理

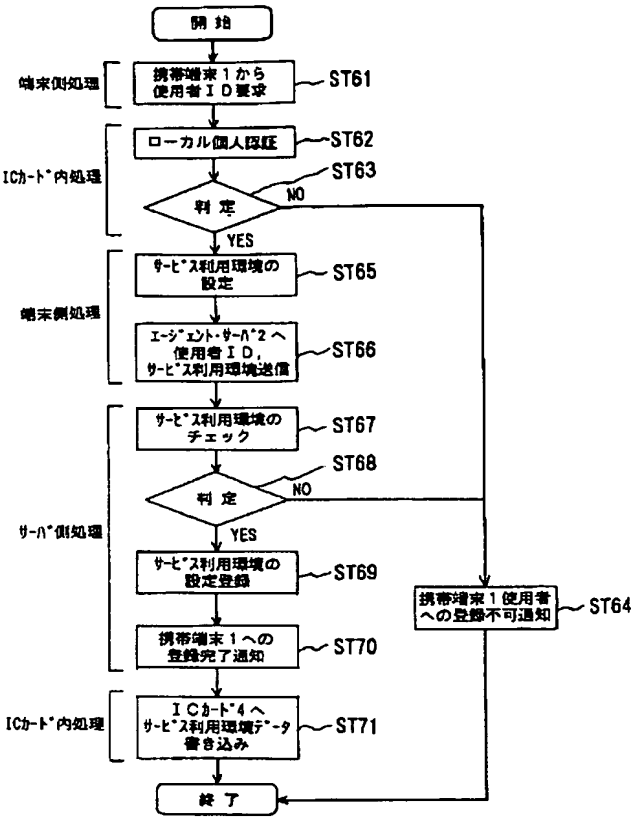
【図８】


開始
携帯端末１から使用者ＩＤ要求
ST51
ローカル個人認証
ST52
判定
ST53
NO
YES
エージェント・サーバ２へ使用者ＩＤ送信
ST55
エージェント・サーバ２で使用者ＩＤチェック
ST56
判定
ST57
NO
YES
エージェント・サーバ２で使用者ＩＤ登録
ST58
携帯端末１への登録完了通知
ST59
ＩＣカード４へサービスＩＤ記入(登録完了)
ST60
携帯端末１使用者への登録不可通知
ST54
終了
端末側処理
ICカード内処理
端末側処理
サーバ側処理
ICカード内処理

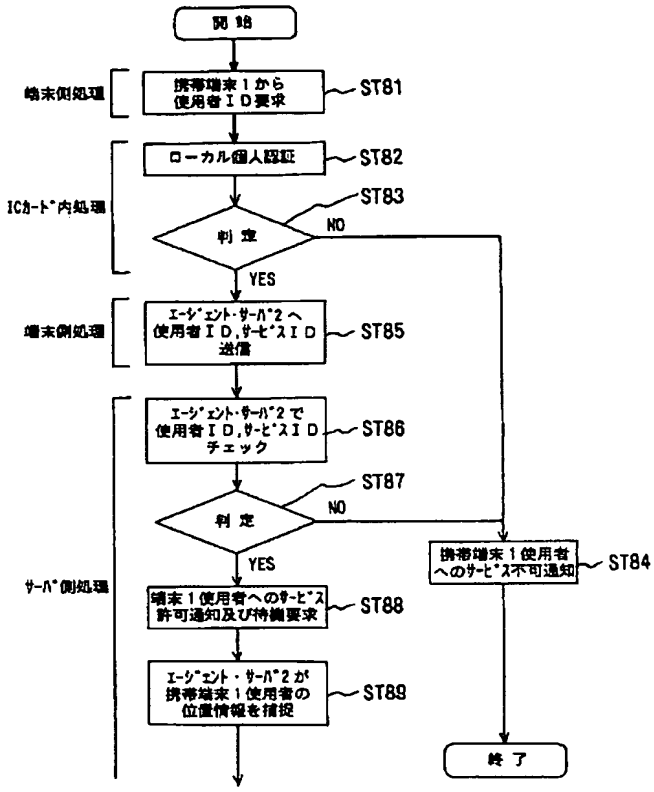
【図１１】


出力情報処理(端末１使用者の現在位置を表す地図情報を作成)
ST90
携帯端末１への処理終了通知
ST91
処理終了通知表示
ST92
ローカル個人認証
ST93
携帯端末１使用者への個人認証要求
ST95
判定
ST94
NO
YES
エージェント・サーバ２から処理結果送信
ST96
処理結果受信・閲覧表示
ST97
エージェント・サーバ２へ受信完了通知
ST98
終了
サーバ側処理
端末側処理
ICカード内処理
サーバ側処理
端末側処理

【図９】



【図１０】



フロントページの続き

(72)発明者　磯村　嘉伯
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　加藤　喜久次
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　酒井　重信
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　斉藤　隆
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　一之瀬　進
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AC01 AE01 AE06 AE12 AE23
AE25 BE01 BG07
5B089 AA16 AA22 AB01 AC03 AD11
AE05 BB09